基于域名共现行为的僵尸网络行为追踪

夏秦，王志文，刘璐
（西安交通大学电子与信息工程学院，710049，西安）

摘要：针对局部行为特征信息偏少而使得僵尸网络行为难以全面追踪的问题，提出了一种基于域名共现行为的僵尸网络行为追踪方法.该方法通过域名共现评分算法计算待测域名与已知僵尸域名的域名共现行为来追踪其他僵尸域名，进而发现更多的僵尸主机；为提高域名评分准确性，还提出了过滤基于网络地址转换的主机域名访问、空间区分单个僵尸网络，以及基于观测时长共现行为统计3项改进措施.采集西安交通大学网络域名服务器的域名查询流量作为数据源进行了实验和测试，结果表明：基于改进的域名评分措施不仅将待测域名数量降为原来的1/4，且计算出的前10名域名共现评分更加合理，提高了追踪僵尸主机的准确性.

关键词：域名共现行为；僵尸网络；网络行为追踪；网络地址转换
中图分类号：TP393 **文献标志码**：A **文章编号**：0253-987X(2012)04-0007-06

Tracking Botnet Activity Based on Co-Occurrence Relation of Domain Name System Queries

XIA Qin, WANG Zhiwen, LIU Lu
(School of Electronics and Information Engineering, Xi′an Jiaotong University, Xi′an 710049, China)

Abstract: Botnet activities can't be tracked entirely with traditional methods because of the deficiency of information in local behavioral feature. A novel approach on tracking Botnet activity is presented based on co-occurrence relation of domain name system(DNS) queries. An algorithm is utilized to calculate the co-occurrence between undetermined DNS and known Botnet DNS so as to find some other Botnet DNS. Three improved measures are proposed in order to increase the accuracy of evaluating co-occurrence. The three measures are filtering DNS access by network address translation, differentiating individual spatial Botnet and observation time based statistic of co-occurrence. Experiments are carried out with test data of DNS queries collected in the campus network of Xi′an Jiaotong University. The results show that some advantages are acquired obviously with the improved measures, such as the number of undetermined DNS can fall to a quarter of traditional method, the co-occurrence acquired is more suitable for the top ten DNS and the accuracy is improved in finding zombies.

Keywords: co-occurrence of domain name; Botnet; tracking in network activity; network address translation

僵尸网络是一群被僵尸程序感染的存在命令与控制关系的僵尸主机集合，这些僵尸主机分布于家庭、企业、政府机构等各种场合，接收来自控制者的指令，执行DDoS、信息窃取、网络钓鱼、垃圾邮件、广告滥点、非法投票等多种网络攻击，作为一种群体性大规模网络攻击手段，对民用互联网、工业生产控

收稿日期：2011-10-27. 作者简介：夏秦(1973—)，女，讲师；王志文(通信作者)，男，副教授. 基金项目：国家自然科学基金资助项目(60970121)；西安市科技计划资助项目(CXY1130①).
网络出版时间：2011-12-29 网络出版地址：http://www.cnki.net/kcms/detail/61.1069.T.20111229.1651.008.html

制系统、军用网络等造成了严重的安全威胁. 一对多的命令与控制(C&C)是僵尸网络区别于传统病毒、木马、后门等攻击技术的根本特点,具有“大规模、有组织、高可控、高隐蔽、长期潜伏”等典型特征.

目前,僵尸网络检测是国内外研究的热点和难点,其主要目的是依据僵尸网络局部特征(如特征码等)发现被控僵尸主机[1-2],近年来也有组织机构研究非特征码检测僵尸网络的方法. 如 Mccusker 等[3]采用网络特征收集分类、主机间威胁和关联性评分,He 等[4]通过域名词法的语义分析在域名中挖掘僵尸域名,Hu 等[5]通过 IP 和域名的 Fast-Flux 现象来检测僵尸网络. 然而,僵尸网络长期潜伏等特点决定了控制者与僵尸主机的交互是一个动态命令与控制过程,导致已知局部特征信息很快被更新,进而检测能力失效. 因此,在控制者的动态控制过程中,如何在局部行为基础上挖掘更多的特征、追踪更多的僵尸网络行为,从而不断获取僵尸网络的全局行为成为深入全面监控僵尸网络的重要问题.

目前,用于检测僵尸网络的局部特征主要为命令与控制服务器的 IP 地址或域名,本文将以命令与控制服务器域名作为已知局部特征,实现对僵尸网络域名访问行为的全方位动态追踪. 在现有的基于僵尸网络域名的研究中,Pittsburgh 大学的 Villamar 等[6]根据异常 DDNS 检测 C&C 服务器,并利用贝叶斯方法通过域名流量的相似性检测僵尸主机,但数据计算复杂,很难应用于大型网络. 为此,本文基于僵尸网络域名共现行为来研究僵尸网络行为追踪,具体包括:①研究了域名共现评分方法的适用范围和缺陷;②提出了一种改进的综合考虑了僵尸网络群体特性和持续性特征的域名共现评分方法,并应用于僵尸网络追踪;③基于真实网络数据验证了所提方法的实施效果.

1 域名共现行为

对于一个给定的域名集合 D 和主机集合 H,在规定的时间范围内若发送给定域名查询的主机又发送了其他域名查询,则称新出现的查询域名所构成的集合 D' 与给定域名集合之间存在域名共现行为,即 $\exists D' \wedge h(D') \subseteq h(D) \subseteq H \rightarrow \mathrm{con}(D', D)$,其中 D' 为共现域名集合,$h(D')$、$h(D)$ 表示向 D' 和 D 发送过域名查询的主机集合. 在大型分布式应用程序中,域名共现行为反映了各参与主机对现有域名的访问规律,为发现新的域名提供了一种关联途径.

通过对近两年捕获到的 Zeus、Srizbi 等 23 例僵尸网络进行长期跟踪分析发现,僵尸网络无论是集中式或分布式结构,均具有如下共性. ①空间上的群体性. 被同一黑客或者黑客组织控制,接收相同或协同的攻击命令,具有相同的网络访问规律. ②时间上的持续性. 僵尸主机在时间上持续访问相关目标服务器,始终保持与僵尸控制者的联系. 僵尸网络在其命令与控制的过程中,通常会使用多个不同域名,且僵尸主机在其生命周期中会持续访问这些特定域名,以便能够持续接收攻击者的命令和控制,并保证自身的隐匿性和可靠性. 图 1 给出了僵尸主机对相关域名的访问过程:首先访问命令控制服务器域名,完成控制命令的接收;随后,访问相关服务器域名,执行更新僵尸程序、下载恶意代码、上传窃取信息等控制命令;最后,访问受害服务器域名,进行网络攻击等. 由于接受同一僵尸控制者控制,同一僵尸网络中的僵尸主机对服务器域名的访问必然存在相同或相似的访问行为.

基于上述分析,可以认定僵尸网络的域名访问具有明显的域名共现行为特征:给定域名集合由已知僵尸域名充当,如捕获所得的命令控制域名,而共现域名集合则涵盖了各种未知僵尸域名,如相关域名和受害域名等.

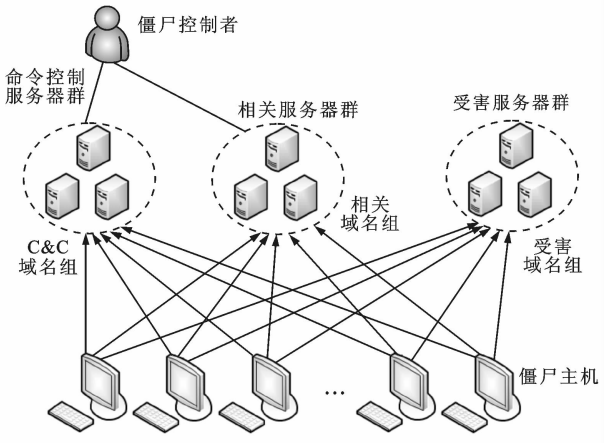

图 1 僵尸网络的域名共现行为

2 基于域名共现行为的僵尸网络行为追踪

基于域名共现行为的僵尸网络追踪方法是通过发现网络中的域名共现行为来达到追踪僵尸网络的目的,该方法面临两个关键问题:①如何发现域名共现行为;②如何凸显面向僵尸网络域名共现行为的特殊性,使之能够区别于其他域名共现行为. 对问题①,可采用域名共现评分方法计算待测域名与已知僵尸域名的共现度,并将共现度较高的待测域名作

为具有域名共现行为的候选域名.对问题②,首先要消除 NAT 主机造成的干扰,然后融合僵尸网络的群体性和持续性特征,从空间维度上细粒度分析单个僵尸网络的域名共现评分特征,从时间维度上连续观测多个时间窗口的域名共现评分特征,使得面向僵尸网络的域名共现行为能够显著区别于面向正常应用的域名共现行为.

2.1　域名共现评分方法分析

Sato 在文献[7]中提出的域名共现评分方法,其核心思想在于当多个主机对一对域名执行了查询,若其中一个域名是恶意的,则另一个域名也是恶意的.但是,在实际网络环境下,通过多次测试,发现该方法存在以下两个问题.

(1) Sato 提出的域名共现评分方法忽略了 NAT 主机的存在,而实验结果表明若存在 NAT 主机,则该方法的置信度和性能都将受到较大影响,具体表现在如下两个方面.①误判的待测域名过多.若 NAT 内网中存在一个访问过感染域名的主机,则内网中所有其他主机访问过的域名都将被判定为待测域名,使得待测域名数量偏高.②给定待测域名的评分不准确.无论 NAT 内网中是否存在访问过感染域名的主机,对于给定的待测域名 d,与之产生域名共现行为的主机数量和僵尸域名数量都与实际情况存在差异,以此为基础计算 d 的共现评分势必会出现较大偏差.

(2)该方法未考虑僵尸网络固有的群体性和持续性特征,使得面向僵尸网络的域名共现行为与面向正常应用的域名共现行为难以区分.由于每个僵尸网络的局部特征各不相同,不能将所有僵尸网络的域名访问行为等同考虑,需要单独考察每个僵尸网络的域名访问,进而扩展其未知僵尸域名.与此同时,僵尸网络域名访问在时间上具有持续性特征,加之各僵尸主机启动时刻的随机性,使得在分析域名共现行为时必须考虑观测时长这一新参数,观测时长越大,对僵尸主机的追踪效果越明显.

2.2　域名共现评分方法的改进

为了更好地追踪僵尸网络的域名访问行为,根据对域名共现评分方法的不足分析,本文进行了 3 方面改进:①过滤 NAT 主机域名访问;②空间粒度细化;③引入观测时长.

2.2.1　*过滤 NAT 主机域名访问*　为了消除 NAT 主机对域名共现行为的影响,最有效的途径就是过滤 NAT 主机的域名访问.由于目前没有明确的 NAT 标识机制,精确的 NAT 主机识别方法均需要特定协议支持,扩展性差.为了充分利用现有域名访问信息,设计了一种简单的基于域名访问统计特性的 NAT 主机识别方法.

设随机变量 X_{ij} 表示主机 i 在第 j($j=1,2,3,\cdots$)个时间周期(如 24 h)内访问的域名数量,其观测值为 x_{ij}.若连续观测了 t 个时间周期,则主机 i 在单个时间周期内访问域名数量的平均值为 $\bar{x}_i=\sum_{j=1}^{t}x_{ij}/t$,若 $\bar{x}_i>M_k$,则认为该主机为 NAT 主机.其中,阈值 M_k 为随机变量 X_{ij} 的上侧 k 分位数,即 $P\{X_{ij}>M_k\}=k, k\in(0,1)$.

2.2.2　*空间粒度细化的域名共现行为分析*　空间粒度细化就是针对单个僵尸网络的域名访问行为独立执行域名共现行为处理.假设已知 N 个僵尸网络的域名特征,每个僵尸网络 B_b 存在 n 个僵尸域名,其集合为 $Z_b=\{d_1,d_2,\cdots,d_n\}$.定义 $R=\{r_1,r_2,r_3,\cdots\}$为 DNS 查询流量数据集,其元素可表示成 4 元组 $r=(t,h,p,d)$,其中 t 表示请求发起时间,h 表示请求发起主机,p 表示请求的资源记录类型,d 表示请求的域名.针对 r 定义获取请求主机和域名的运算符 $\Phi(r)$和 $\Gamma(r)$,若一个主机向 Z_b 中任一域名发出过 DNS 查询请求,则将该主机定义为僵尸网络 B_b 的僵尸主机,其集合表示为 $H_b=\{h_1,h_2,\cdots,h_m\}$,即

$$\forall h\in H_b\rightarrow\exists d\in Z_b\wedge\exists r\in R\wedge\Phi(r)=h\wedge\Gamma(r)=d$$

将僵尸网络 B_b 中主机访问的未知域名定义为共现行为待测域名集合 $C_b=\{d_1,d_2,\cdots,d_k\}$,即

$$\forall d\in C_b\rightarrow d\notin Z_b\wedge\exists h\in H_b\wedge\exists r\in R\wedge\Phi(r)=h\wedge\Gamma(r)=d$$

僵尸网络 B_b 中待测域名 d 的共现评分 $S_b(d)$ 定义为

$$\left.\begin{aligned}S_b(d)&=\Big(\sum_{d_b\in Z_b}C(d_b,d)\Big)W(d)\\C(d_i,d_j)&=\frac{\sum\limits_{\{h\mid d_i\in D_h\wedge d_j\in D_h\}}1/\mid D_h\mid}{\mid\{h\mid d_i\in D_h\vee d_j\in D_h\}\mid}\\W(d)&=\frac{\mid\{h\mid h\in H_b\wedge d\in D_h\}\mid}{\mid\{h\mid h\in H\wedge d\in D_h\}\mid}\end{aligned}\right\}\quad(1)$$

根据式(1),计算与僵尸网络 B_b 对应的待测域名集合 C_b 的所有域名共现评分,选取分数较高的若干域名作为 B_b 的僵尸域名.

2.2.3　*基于观测时长的域名共现行为分析*　从时间持续性这一特征来判定待测域名是否为僵尸域名,将观测时长划分为若干个等时长的时间窗口,若

存在多个时间窗口,使得待测域名与已知僵尸网络域名共现评分较高,则该域名是未知僵尸域名的可能性较大.

设时间窗口大小为 T,对每个时间窗口 t,分别应用式(1)计算待测域名 d 与僵尸网络 B_b 的共现评分 $S_b(d,t)$,则在 x 个连续时间窗口中,可以得到域名 d 与僵尸网络 B_b 的共现评分集合 $S(d,B_b)=\{S_b(d,t_1),S_b(d,t_2),\cdots,S_b(d,t_x)\}$,计算域名 d 与僵尸网络 B_b 的平均共现评分 $\overline{S}_b(d)=(S_b(d,t_1)+S_b(d,t_2)+\cdots+S_b(d,t_x))/x$,并取域名 d 与僵尸网络 B_b 的最大共现评分 $S_{bmax}(d)=\max(S_b(d,t_i))$. 在计算中引入观测时长的域名共现评分 $S_b(d)$时,定义 $S_b(d)$为

$$S_b(d)=\frac{\overline{S}_b(d)}{\max(\overline{S}_b(d_i))}\alpha+\frac{S_{bmax}(d)}{\max(S_{bmax}(d_i))}(1-\alpha) \tag{2}$$

式中:$\max(\overline{S}_b(d_i))$为僵尸网络 B_b 所有待测域名平均共现评分的最大值;$\max(S_{bmax}(d_i))$为僵尸网络 B_b 所有待测域名最大共现评分的最大值;$\alpha\in(0,1)$为反映网络中域名共现评分平均值与最大值比例的比例因子. 在基于观测时长的域名共现行为分析中,时间窗口 T 直接反映了僵尸网络的持续性特征,其取值受两个因素影响:①僵尸主机数量,若僵尸主机数量占主机总数的比例较大,则可认为在任何时间都存在稳定数量的在线僵尸主机,此时 T 值可以偏小;②待测僵尸网络中僵尸主机与僵尸控制者间的联系频率,若联系频率较高,T 的取值可以较小.

3 验证与分析

3.1 数据采集与预处理

如图 2 所示,通过西安交通大学网络中心取得西安交通大学域名服务器入口的数据包镜像流量(约 4 Mb/s),提取 DNS 查询流量中包含 DNS 查询特征信息的 4 元组 $r=(t,h,p,d)$,得到初始数据集 R. 经过一年多的数据采集,发现在每天采集的约 8 300万条数据记录中,绝大多数是正常 DNS 查询. 为适应大规模网络,提高域名共现计算的处理性能,有必要对初始数据执行数据约简和数据统计预处理.

3.1.1 *数据约简* 通过"域名白名单"过滤来约简数据集,不仅可将数据量降低到 1 600 万条/d,而且排除了大量噪声数据. "域名白名单"是指与僵尸网络检测和分析无关的域名,主要包括常用域名、错误配置域名以及程序频发域名 3 种.

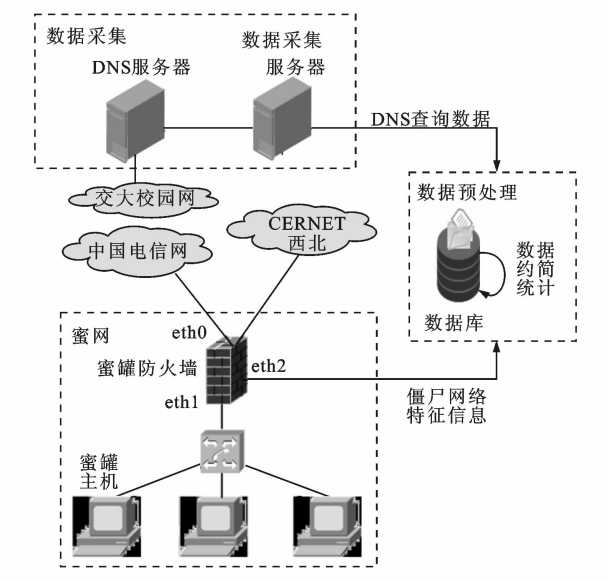

图 2 数据采集网络拓扑

3.1.2 *数据统计* 基于约简后的数据集针对域名执行统计处理,统计 $R=\{r_1,r_2,r_3,\cdots\}$中每个域名每天的查询主机数量分布得到数据集 $R_s=\{s_1,s_2,s_3,\cdots\}$,其元素也是 4 元组 $s=(t,h,d,n_{all})$,其中 n_{all} 表示域名 d 在日期 t 被主机 h 查询的总次数. 数据统计能够在不丢失有效信息的情况下将每天采集的数据降低至 350 万条.

3.2 实验分析

3.2.1 *NAT 主机对域名共现评分的影响* 假定存在 15 个僵尸域名(5 个已知 10 个未知)、10 个僵尸主机,对 NAT 网络中僵尸主机数量为 0、1、5 和 10 的 4 种情况进行了实验. 为了使仿真更接近真实网络,充分考虑到僵尸主机可能因为网络连通性、程序冲突、系统稳定性等原因未能访问所有僵尸域名,故仿真僵尸域名访问数据生成规则定义为:随机在非 NAT 主机和 NAT 主机选取相应数量的主机,使每个主机随机访问 15 个僵尸域名中 3 个以上数目的域名,即认为加入若干数据记录 $r=(t,h,p,d)$,其中主机 h 和域名 d 按照上述规则设置.

通过实验计算待测域名的域名共现评分,并借用式(2)取比例因子 α 为 0 对评分结果做归一化,使其值分布在[0, 1]之间. 当网络中存在 NAT 主机时,若 NAT 主机内存在僵尸主机,则:①排除 NAT 主机域名访问前后的待测域名数量相差悬殊(接近 4 倍之多),结果如表 1 所示;②在不排除 NAT 主机域名访问情况下,NAT 网络中其他主机产生的噪声数据使得域名共现评分获得的僵尸域名置信度无法保证,且评分方法的置信度随NAT主机中僵尸主

表 1　待测域名数

NAT 主机	待测域名数	
	过滤 NAT 主机	不过滤 NAT 主机
0	148	148
1	1 204	7 892
5	152	7 614
10	1 288	7 494

注:NAT-Host 表示 NAT 网络包含的僵尸主机数目.

机数目增多大幅度下降,如表 2 所示. 极端情况下,即 10 个僵尸主机全部分布在 NAT 网络中时,发现存在 1 317 个域名评分相等且为最高评分,此时的评分方法将失去意义. 事实上,处于同一 NAT 子网内的主机感染同一恶意程序的可能性比分布在不同子网上的主机更大.

表 2　评分前 10 名的僵尸域名数

NAT 主机	评分前 10 名的僵尸域名数	
	过滤 NAT 主机	不过滤 NAT 主机
0	10	10
1	10	10
5	10	7
10	10	0

3.2.2　*改进的域名共现评分方法与原方法比较*　利用图 2 的蜜网环境捕获到的僵尸域名进行实验,选取僵尸主机较多的一个僵尸网络 B_1,其已知僵尸域名为{ircd. zief. pl, proxim. ircgalaxy. pl, proxima. ircgalaxy. pl}.

对时间窗口 T,考虑到教育网僵尸主机数量不大且其与命令控制服务器联系存在时差问题,实验中取值尽可能大,设置为 1 d;同时考虑到教育网用户具有一定的安全防范意识,对比例因子 α 取值为 0.8,NAT 网络的识别参数 k 取值为 0.95.

在计算待测域名的共现评分 $S_1(d_i)$ 时,发现 $S_1(d_i)$ 的概率累积分布超过 95% 的待测域名的共现评分都小于 0.2,因此只需要关注那些共现评分超过 0.2 的域名即可. 本文计算了原域名共现评分 $S(d_i)$,借用式(2),设比例因子 α 为 0,与改进的评分方法进行了对比,结果如表 3 所示.

由表 3 可以得出下述结论:①改进后的待测域名数量较改进前大幅度减少,降低了计算量;②改进后的域名共现评分方法,评分大于 0.2 的域名 35 个,僵尸域名占 42.9%,原评分方法评分大于 0.2 的域名 53 个,僵尸域名占 37.7%,两种方法检测结果中重叠的僵尸域名 13 个,改进后的方法检测结果中没有原方法检测结果中的 7 个域名,其原因是这些域名仅在一个时间窗口中出现且只与一个僵尸主机相关,而这与僵尸网络的群体性和持续性特征并不相符;③改进后的域名共现评分结果中,评分相同的域名类型相同,而原域名共现评分结果中,评分相同的域名中既存在僵尸域名也存在正常域名,如评分同为 0.736 5 的 18 个域名中存在僵尸域名 6 个、正常域名 12 个,这个结果表明改进后的评分方法对域名相关性的表现力更强,与僵尸网络的群体性特征更加相符.

表 3　两种域名共现评分方法对比

改进后的评分方法(待测域名数:2 115)			原评分方法(待测域名数:25 383)		
评分值	域名个数	域名类型	评分值	域名个数	域名类型
1	1	恶意	1	1	恶意
0.948 5	1	恶意	0.736 5	6	恶意
0.891 1	5	恶意	0.736 5	12	正常
0.791 7	1	恶意	0.672 1	5	恶意
0.570 8	2	恶意	0.499 2	1	恶意
0.483 0	17	正常	0.263 4	7	恶意
0.393 2	3	正常	0.263 4	19	正常
0.305 2	4	恶意	0.245 5	2	正常
0.247 8	1	恶意			

在上述两种评分方法对比中,对共现评分超过 0.2 的待测域名均采用如下规则来判定其是否真的具有恶意性:

(1)安全厂商公布该域名为僵尸域名或该域名下存在恶意 URL;

(2)和已知僵尸域名具有相同的二级域名,且该二级域名不是动态域名提供商;

(3)和已知僵尸域名具有相同的前缀;

(4)通过搜索引擎发现没有该域名的信息,但它的确存在,且解析所得 IP 地址与已知僵尸域名解析的 IP 地址相同.

3.2.3　*域名共现评分方法的影响因素分析*　影响域名共现行为效果的主要因素有 3 个,即已知僵尸域名数、现有僵尸主机数以及僵尸主机在线时长. 对于给定的僵尸网络,若已知僵尸域名个数与现有僵尸主机数越多,则其空间群体性特征越突出,通过域

名共现行为分析得出的僵尸网络域名访问行为置信度越高;同时,若僵尸主机在线时长越大,则僵尸主机与控制者交互的概率越大,其时间持续性特征越明显,所获得的僵尸网络域名访问行为置信度越高.实验中恰好发现存在一个僵尸网络,其校园网内僵尸主机数目为1,由于该网络域中包含僵尸主机数过少,僵尸网络空间特性不明显,虽追踪出了5个僵尸网络域名,但同时也包含了13个正常域名,未能达到追踪僵尸网络域名访问行为的目的.

4 结束语

本文针对Sato提出的域名共现评分的缺陷和不足,提出了消除NAT主机对域名共现评分机制追踪僵尸网络的新方法;对僵尸网络的空间维度作了进一步的粒度细化分析,将不同僵尸网络行为区分开来,同时引入了时间维度的评分分析.以西安交通大学校园网的实际DNS查询流量为数据源进行了僵尸网络追踪,实验结果表明改进的域名共现评分方法能够更好地识别僵尸域名,为追踪感染主机提供了有效的参考依据.

由于本文所提的域名共现行为要求僵尸网络的域名特征具有一定的稳定性,但实际上有些僵尸网络的域名特征变换非常频繁(如Conficker),从而难以捕获到有效的域名共现行为.为此,下一步研究工作拟将本方法扩展到基于主机共现行为的僵尸网络行为追踪,使之能够适用于更多的僵尸网络.

参考文献:

[1] KONRAD R, GUIDO S, TOBIAS L, et al. Detecting the phoning home of malicious software [C]// Proceeding of the 2010 Symposium on Applied Computing. Los Alamitor, CA, USA: IEEE Computer Society, 2010:298-304.

[2] PETER W, LEYLA B, THORSTEN H, et al. Automatically generating models for Botnet detection[C]// Proceeding of Symposium on Research in Computer Security. Los Alamitos, CA, USA: IEEE Computer Society, 2009:104-110.

[3] MCCUSKER O, KIAYIAS A, WALLUCK D, et al. A combined fusion and mining strategy for detecting Botnets [J]. International Journal of Information Security, 2009, 8(11):71-82.

[4] HE Yuanchen, ZHONG Zhenyu, TANG Yuchun. Mining DNS for malicious domain registrations [J]. Journal of the ACM, 2010, 12(32):335-348.

[5] 胡欣, 沈涛. 僵尸网络全局IP使用模式测量与分析[J]. 计算机学报, 2011, 34(2): 207-214.
HU Xin, SHEN Tao. Measurement and analysis of global IP-usage patterns of Botnets [J]. Chinese Journal of Computers, 2011, 34(2): 207-214.

[6] VILLAMAR R, BRUSTOLONI J C. Identifying Botnets using anomaly detection techniques applied to DNS traffic [C]// Proceeding of the 5th IEEE Consumer Communications and Networking Conference. Los Alamitos, CA, USA: IEEE Computer Society, 2008:476-481.

[7] SATO K, ISHIBASHI K. Extending black domain name list by using co-occurrence relation between DNS queries [C]// Proceeding of the 2010 USENIX Workshop on Large-Scale Exploits and Emergent Threats. Los Alamitor, CA, USA: IEEE Computer Society, 2010:2011-2020.

[本刊相关文献链接]

应用部分马尔科夫博弈的网络安全主动响应决策模型. 2011,45(4): 18-24.
使用交叉熵检测和分类网络异常流量. 2010,44(6):10-15.
网络结构鲁棒性指标及应用研究. 2010,44(4):93-97.
一种面向传感器网络的蚁群优化路径恢复算法. 2010,44(1):83-86.
最大化网络有效寿命的传感器网络覆盖保持协议. 2009,43(10):66-70.
一种相邻节点协作的无线传感器网络可靠传输方案. 2009,43(2):33-37.
网络安全协同防卫系统研究与实现. 2008,42(12):1495-1499.
利用最大似然准则的双向联想网络研究. 2008,42(12):963-966.
一种面向网络行为因果关联的攻击检测方法. 2008,42(8):931-935.
无线传感器网络低时延能量均衡安全路由. 2008,42(2):161-165.

(编辑 荆树蓉)